



NZX Cyber security

Security and Reliability Council – Electricity Authority
October 2023

▶ New Zealand's Exchange
Te Paehoko O Aotearoa



NZX's history goes back to the first gold exchange established in Otago in 1866. Further exchanges were established around other parts of the country culminating in the Stock Exchange Association in 1915. The regional model was consolidated in 1991 and in 2003 NZX listed on the main board and an independently governed board was established. The New Zealand Stock Exchange also formally changed its name to NZX.

Today, NZX operates New Zealand's equity, funds, derivatives, energy and carbon markets. To support the growth of our markets, we provide trading, clearing, settlement, depository and data services for our customers. We also have a funds management business Smartshares and advisory platform NZX Wealth Technologies.

In terms of supervision, NZX is currently the most regulated firm in Aotearoa with not just governmental and regulatory, but industry bodies such as SWIFT for payment and clearing systems also having security and risk frameworks we are required to adhere to as a condition of use.

2020 – Distributed Denial of Service (DDoS)

Prior to August 2020, NZX had embarked on a program of network modernisation. This involved:

- Upgrades of perimeter technologies
- Introduction of new capabilities
- Upgrades of core networking and architecture

In terms of external protections, what was in place was reasonable with vulnerability scans of the perimeter, WAFaaS in place and considerably more powerful perimeter firewalls.

Threat intelligence from both government intelligence agencies and sector partners had (in retrospect) indicated that “malicious actors” were ramping up interest in disrupting New Zealand infrastructure.

DDoS floods a targets internet connection with traffic so as to make it unusable for legitimate use. In August of 2020 a cyber-attack using DDoS was carried out against NZX. This was highly visible in the NZ media and disrupted NZX’s business.

Capital Markets were disrupted due to the inability to publish market information (NZ regulatory requirement out of step with other trading regulatory obligations. However, trading was still up, and possible as capital markets connectivity is not carried over the Internet.

In a similar vein, NZX Electricity market websites were not available to the Internet. Big 5 utilise private connections like the capital markets.

The network modernisation enabled the deployment of added protective capabilities including big uplifts in Internet shielding.

Outcomes

Technology and Cyber

The resultant disruption led to a review of NZX technology and cyber capabilities by the Financial Markets Authority (FMA).

The FMA produced several recommendations (as obligations) broadly summarised as:

- NZX needed to improve its cyber resilience capability and onboard specialist resource to guide this. This included the implementation of Security Operations Centre and SIEM technology
- Improvements in risk management practices – especially relating to technology and cyber risk.
- Improvements in responsiveness regarding its incident response.
- Increase NZX's interaction with other entities around NZ and industry to improve situational awareness of cyber threats.

Governance and Regulation

Some regulatory changes were also developed:

- Increased scrutiny and oversight of NZX operations by the regulator.
- Change to the regulatory requirement for Market Announcements to be available online as a condition of the markets being open.

Cyber - approach

July 2021 led to the onboarding of new Head of Information Security for NZX.

Early priorities were:

- Review existing capabilities through a lens of People>Process> Technology
- Review existing risks and obligations
- Identify business priorities and how these drive cyber priorities
- Identify issues that needed to be tackled quickly and build a view of priority action (taking into account all of the above).

Initial Activities

Initial review of DDOS protections yielded Internet facing sites built post-attack had not been fully implemented behind the shielding.

Existing known web vulnerabilities while shielded, had not been addressed.

Review of malicious code (legacy term “anti-virus”) tools showed 3 solutions in place with some systems having none of the 3 installed

Technology risk registers did not use risk language to articulate business risk. Example being DDOS and its likelihood vs impact ratings. Updating of the risk registers was implemented in tandem with the arrival of a GM of Enterprise Risk that better measured out tech and cyber risk and gave leadership a clearer picture of priorities

NIST Cyber Security Framework had been previously selected as the mechanism for measuring cyber-maturity. A review of NIST posture was already underway in 2021. Early finding was that the maturity was being measured inconsistently across the organisation.

The network modernisation project had included the implementation of a Security Incident Event Manager (SIEM) software solution and accompanying Security Operations Centre (SOC). This was also part of the FMA obligations with a due date of operationalisation by Xmas 2021.

Action

Unshielded sites were quickly remediated. Any site sitting on the same circuit as an unshielded one is vulnerable to an attack on the unprotected one. NZX (along with many other NZ FSI's and Nationally Significant Organisations) was attacked in August 2021 by the same actors who attacked in 2020.

Web vulnerabilities were fixed (procedural issue) and then continuous monitoring of any exceptions going forward to ensure anything identified is dealt with promptly. We haven't reported an exception to the board in over a year now!

After a quick assessment, the right fit anti-virus (out of the 3 existing solutions) was selected and a light touch project was initiated to remove the other two and fully deploy the desired one. Coverage taken from 40% of endpoints to 100% (a few exceptions were noted) using a best of breed Extended Detection and Response (XDR) with outsourced 24/7 monitoring.

All risk registers were updated and used to inform action plans across technology.

NIST reviews were re-baselined with a consistent criteria. In some cases, this led to a downgrading of perceived maturity for some capabilities. This was a positive as it demonstrated that we had a better understanding of where we were.

SOC/SIEM project was incepted August 2021 with delivery of a Minimum Viable Product (core networks and core user directory) 1 week before Xmas.

Ongoing journey

While the early driver was FMA obligations, we have never lost sight of the fact that NZX is an enterprise with business units other than just the Capital Markets.

Our energy and electricity market footprint benefits from the same approach as the capital markets. An enterprise is only as strong as its weakest link. So we utilise the same best of breed cyber protective/detective capabilities for our Electricity markets as we do for our Capital markets.

The program tackles risk through a lens of 'everything has NZX above the door'.

However...the market operator obligations for clearing and settlement follow NIST CSF so it's a convenient intersection to shape our cyber work.

People > Process > Technology

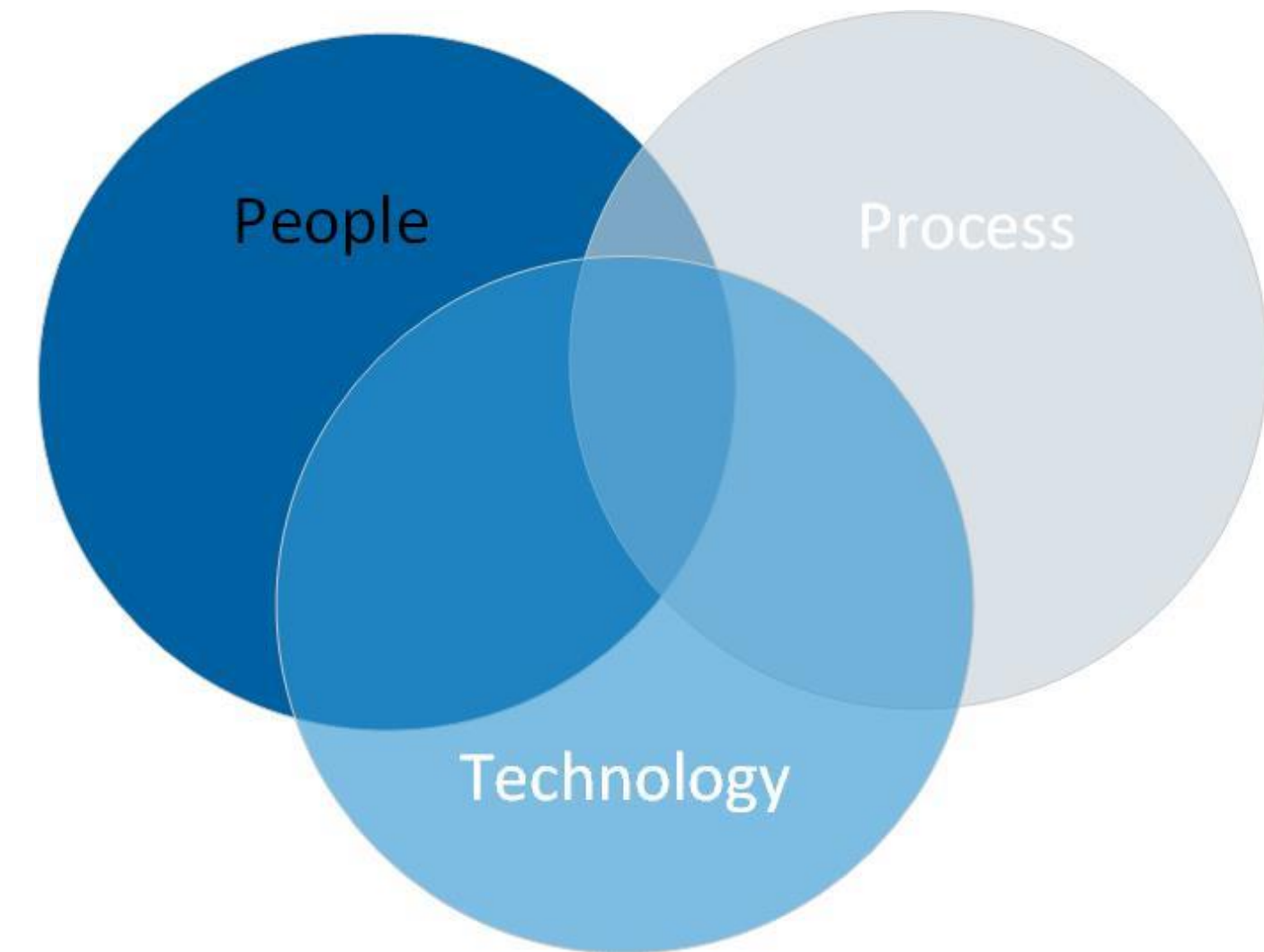
People

Arguably the most important part of the triad, without this, we can't execute process or deploy technology.

While, like many other organisation we deploy cyber awareness training to our workforce we also;

Hold quarterly phishing tests (results reported to the board). A Key Risk Indicator, if we go above a certain percentage of clicks, we have to review our approach and whether we need to change anything.

Education sessions: We have sessions on cyber risk and capabilities with directors and executives. Those owning the risk need to have a clear view of how it is shaped and whether we are doing the right things (or not!).



People > Process > Technology

People

NZX Security team is small (but with a large impact!). To cover the ground that we do we;

- Technology staff have regular learning sessions on security tooling and capabilities as well as learning materials for secure development which is being expanded out across the organisation in 2024 so that we have more people thinking about security objectives and help with some of the tech.
- Have strategic partners to help with eyes-on-glass for key operational systems
- Have strategic partners to with some of the overflow on business advisory and other operational matters such as security testing

People > Process > Technology

Process

Governance – The NZX board receives regular reporting on cyber risk, key initiatives and progress updates and any major status changes in risk as well as updates on the threat landscape that NZX is operating in.

Quarterly Cyber committee with technology leadership and business stakeholders that informs direction and provides a valuable feedback mechanism for ensuring business drivers are considered as part of cyber strategy.

Assurance – Monthly risk forums are held between technology and 2nd line risk to ensure we are constantly re/measuring risk and actions are being undertaken and followed up.

Reporting –activities, insights and analytics all need to be actionable. If a report is being generated, it needs to serve purpose for someone to do something.

Incident Response – An important part of the NIST framework and a key learning from the events of 2020 was the need for not only having a plan for how to respond in an emergency, but also that it is relevant, up-to-date and practiced (so you can identify

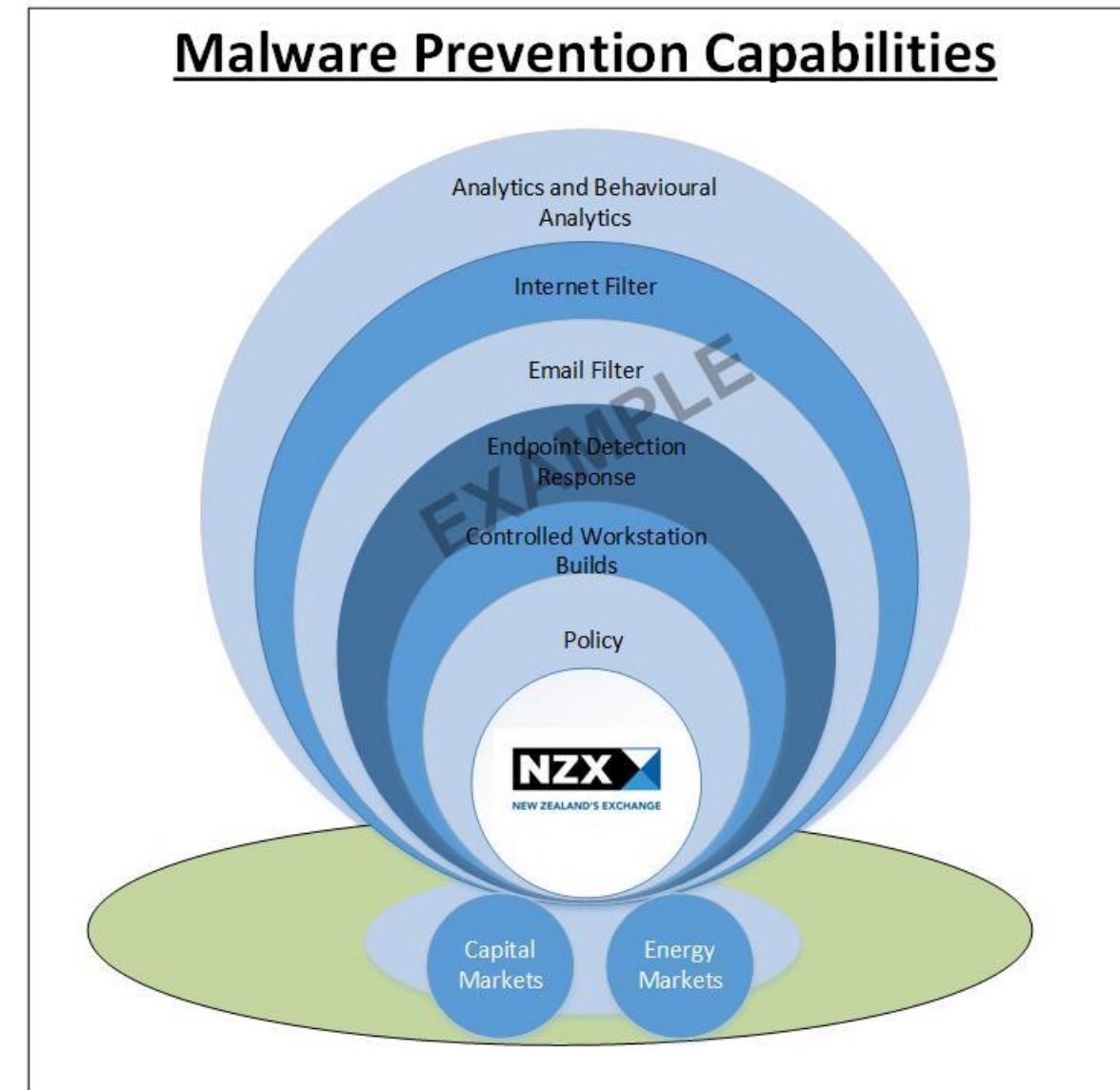
People > Process > Technology

Process

Architecture – we have built a capability architecture where we look for what detective/protective capabilities are in place to mitigate each identified risk.

This model covers People>Process>Technology and helps us to contextualise where we may have gaps and communicate these to our executive and directors.

For each layer we look at the effectiveness, maturity and coverage of each control to inform how well we are addressing risks.



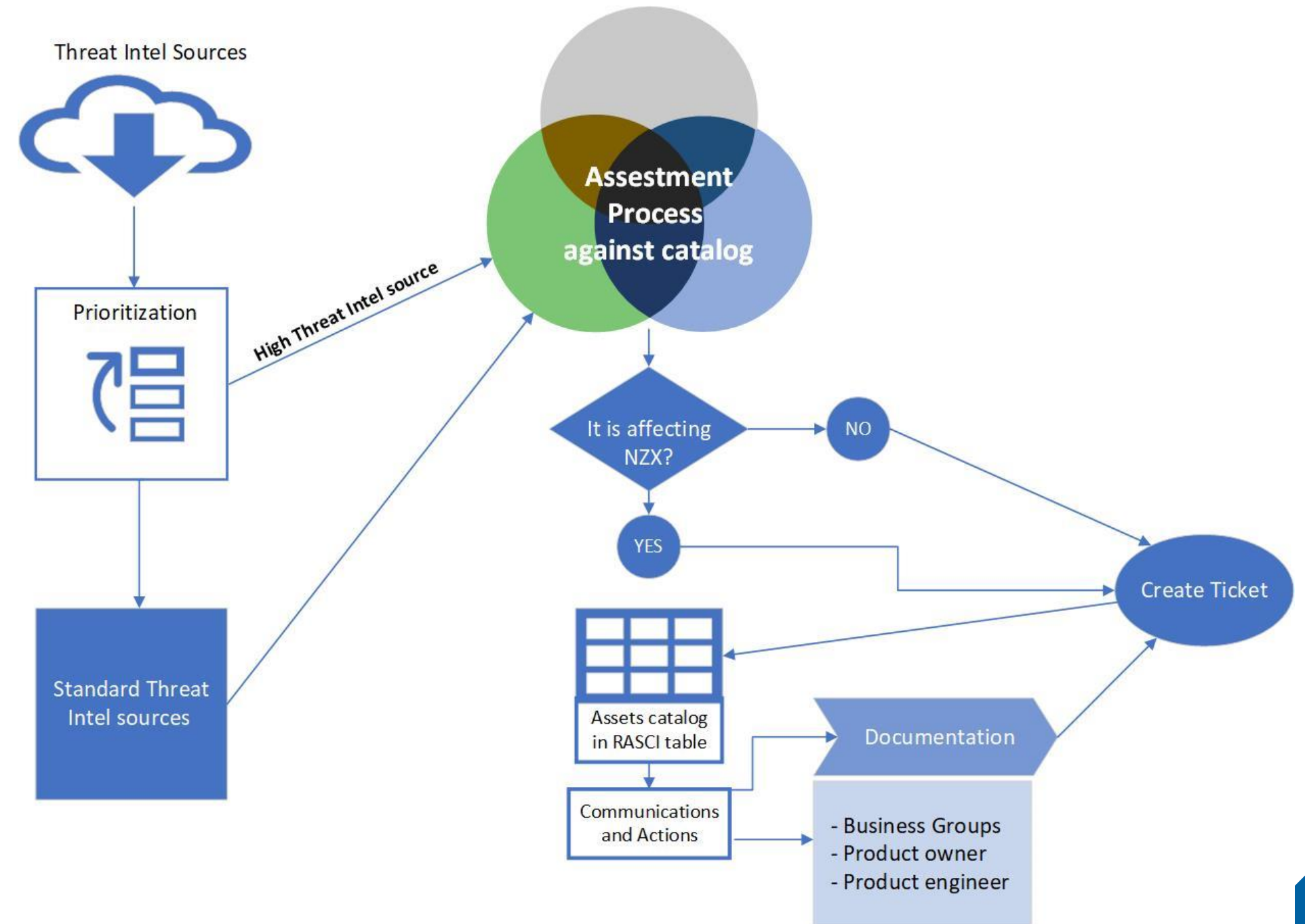
People > Process > Technology

Process

Threat Intelligence and incident response – The findings from 2020 recommended that NZX improve its situational awareness and its ability to cope with incidents. We drive a lot of our via threats, our ability to proactively deal with threats before they affect us is critical to ensuring our safety.

NZX now:

- Has a number of governmental and (finance) industry threat feeds that allow us to proactively address emerging threats faster. We also automate the feed of some of these into our telemetry systems.
- Has regular incident response workshops, exercises and training to improve match fitness



People > Process > Technology

Technology

While Cybersecurity has a deep technological component the security function works closely with the technology teams to help with building roadmaps and the prioritisation of risk mitigations. Technology roadmaps that ensure systems are up to date with supported technology improve our security, reduce risk and are operationally more efficient to maintain. Security is a full team effort, not just the responsibility of the security team.

NZX utilises the defence-in-depth approach to addressing its risks (illustrated via the 'onion' model) to ensure we have multiple layers of safeguards in place to address potential threats and vulnerabilities. The focus is on detect and protect.

We have 24/7 monitored coverage of:

- Internet shielding including Web application firewalls
- Platforms (e.g. servers, networks, cloud platforms)
- Extended Detection and Response (antivirus)

We also run behavioural analytics and threat hunt analytics, patch intelligence etc to complement the detective and protective capabilities.

Key Thematic Lessons From NZX's Journey

1. Understanding and being able to measure (even qualitatively) your risks gives you the best means of prioritising your activities (=spend)
2. Its not just an “IT issue”. The impacts are to the business itself. The business needs to be a part of the prioritisation process (see point 1.)
3. It's a full team effort. IT should work with security to help prioritise risk mitigation activities (see point 1.) with the business owners (see point 2!)
4. Focus on visibility and coverage, having monitoring or protective capabilities on half your systems will result in the compromise occurring where you can't see (or do).
5. Use the defence-in-depth approach where you can. Measure your effectiveness and tie it to your risks so you are investing your time, effort and dollars on the right things



Moving Forward

1. We are continuing with the maturation of existing capabilities (e.g. SIEM monitoring, XDR)
2. Cyber risk is now a tier 1 risk separate from Technology risk. So greater measurement, scrutiny and reporting
3. Addition of more capabilities that we identified via the onion model approach
4. Adding more automation to response capabilities
5. Continuing Incident Response exercises and training

The background is a solid blue color. In the top-left corner, there is a dark blue triangle pointing towards the center, with a light grey triangle above it. In the bottom-right corner, there is a dark blue triangle pointing towards the center, with a light green triangle below it.

Questions?

Thank you

The information provided is a guide only and intended for general information purposes. It does not constitute investment advice. Any representation or statement expressed in this information is made in good faith on the basis that NZX Limited (NZX) or any of its related companies is not able to be liable in respect of such representation or statement arising in any way including from any error or omission. This information should not be relied upon as a substitute for detailed advice from an authorised financial adviser. NZX does not guarantee the accuracy and/or completeness of the information, or the accuracy of third-party information. NZX assumes no responsibility to update this report after publication. Except for any liability which cannot be excluded, NZX, its directors, officers, employees and agents disclaim all liability for any error, inaccuracy or omission, or any loss suffered through relying on this report. All information provided is confidential in nature and is imparted in confidence. As such, the information should not be disclosed to any other person. No part of this information may be redistributed or reproduced in any form or by any means without the written consent of NZX. Copyright © NZX Limited.